

APPENDIX A

```
5      IF (it is time to perform housekeeping activities) THEN
       FOR (each TCP connection that has started to close, i.e. observed the TCP FIN flag set) DO
         IF (the time allowed for closure has passed) THEN
           Close this connection

         IF (this is the last connection with this user) THEN
           Reinitialize the user's profile and set the profile state to Incomplete
         ENDIF
       ENDIF
     NEXT

10     FOR (each connection that has been idle for the maximum allowed time) DO
     Close this connection

     IF (this is the last connection with this user) THEN
       Reinitialize the user's profile and set the profile state to Incomplete
     ENDIF
   NEXT
ENDIF

15     FOR (each connection that has been idle for the maximum allowed time) DO
     Close this connection

     IF (this is the last connection with this user) THEN
       Reinitialize the user's profile and set the profile state to Incomplete
     ENDIF
   NEXT
ENDIF

20     IF (it is an IP packet) THEN
       IF (it is an IP/UDP packet) THEN
         Check the source and destination ports against a list of allowed well-known UDP ports
       ELSE
         IF (either port is on the allowed port list) THEN
           IF (the server port is for the XDMCP protocol) THEN
             Check the XDMCP Opcode against a list of allowed opcodes
           ELSE
             IF (the XDMCP Opcode is on the allowed opcode list) THEN
```

Check if the XDMCP packet is being sent in an allowed direction

35 IF (an allowed Opcode is being sent to the server or an allowed Opcode is being sent to the user) THEN
 IF (there is an established X-Windows connection with this user) THEN
 IF (the Opcode is other than KeepAlive or Alive) THEN
 Discard the packet
 ENDIF
 ELSE
 IF (the Opcode is KeepAlive or Alive) THEN
 Discard the packet
 ENDIF
 ENDIF
 ENDIF
 45
 Create and initialize a profile for this user
 Set the profile state to Incomplete
 IF (the Opcode is Query) THEN
 Reinitialize the user's profile and set the profile state to Incomplete
 FOR (each Authentication Name in the packet) DO
 IF (the Authentication Name is not recognized) THEN
 Discard the packet
 ENDIF
 NEXT
 Remember the Authentication Names in the user's profile
 ELSE IF (the Opcode is Willing) THEN
 IF (the Authentication Name in the packet is not recognized) THEN
 Discard the packet
 ENDIF
 ENDIF
 60

65

IF (the Authentication Name is not one of the authentication names recorded in the user's profile from the Query packet) THEN
 Discard the packet
ENDIF

70

Remember this Authentication Name in the user's profile

IF (the Hostname supplied by the server is NOT syntactically valid) THEN
 Discard the packet
ENDIF

75

IF (the Status string is NOT composed of printable characters) THEN
 Discard the packet
ENDIF

80

ELSE IF (the Opcode is Unwilling) THEN
 IF (the Hostname supplied by the server is NOT syntactically valid) THEN
 Discard the packet
 ENDIF

85

IF (the Status string is NOT composed of printable characters) THEN
 Discard the packet
ENDIF

90

Reinitialize the user's profile and set the profile state to Incomplete

ELSE IF (the Opcode is Request) THEN
 IF (the X Display Number is invalid) THEN
 Discard the packet
 ENDIF

95

Remember this Display Number in the user's profile

```
FOR (each Connection Type in the packet) DO
  IF (the Connection Type is not IP) THEN
    Discard the packet
  ENDIF
NEXT

105
FOR (each Connection Address in the packet) DO
  IF (the Connection Address is not an IP address) THEN
    Discard the packet
  ENDIF
NEXT

110
IF (the Connection Address does not match the user's IP address) THEN
  Replace the Connection Address with the user's IP address
ENDIF
NEXT

115
IF (none of the Connection Addresses matched the user's IP address) THEN
  Discard the packet
ENDIF
NEXT

120
IF (the Authentication Name in the packet is not recognized) THEN
  Discard the packet
ENDIF
NEXT

125
IF (the Authentication Name does not match the Authentication Name recorded in the user's
profile from the Willing packet) THEN
  Discard the packet
ENDIF
```

authentications. If the lengths of the Authentication Name and Authentication Data are not both zero or non-zero) THEN
Discard the packet
ENDIF

FOR (each Authorization Name in the packet) DO
 IF (the Authorization Name is not recognized) THEN
 Discard the packet
 ENDIF
NEXT

Remember the Authorization Names in the user's profile

130
135
140
145
150
155

IF (if the Manufacturer Display ID contains invalid characters) THEN
 Discard the packet
ENDIF

IF (if the Manufacturer Display ID does not match any previous recorded Display ID for this user) THEN
 Discard the packet
ENDIF

ELSE IF (the opcode is Accept) THEN
 Remember the Session ID in the user's profile
 IF (the Authentication Name in the packet is not recognized) THEN
 Discard the packet
 ENDIF

 IF (the Authentication Name does not match the Authentication Name recorded in the user's profile from the Request packet) THEN
 Discard the packet

160 ENDIF

161 IF (the lengths of the Authentication Name and Authorization Data are not both zero or non-zero) THEN

162 Discard the packet

163 ENDIF

164 IF (the Authorization Name in the packet is not recognized) THEN

165 Discard the packet

166 ENDIF

167 IF (the Authorization Name does not match any of the Authorization Names recorded in the user's profile from the Request packet) THEN

168 Discard the packet

169 ENDIF

170 Remember the Authorization Name in the user's profile

171 IF (the lengths of the Authorization Name and Authorization Data are not both zero or non-zero) THEN

172 Discard the packet

173 ENDIF

174 ELSE IF (the opcode is Decline) THEN

175 IF (the Status string is NOT composed of printable characters) THEN

176 Discard the packet

177 ENDIF

178 IF (the Authentication Name in the packet is not recognized) THEN

179 Discard the packet

180 ENDIF

181 190

IF (the Authentication Name does not match the Authentication Name recorded in the user's profile from the Request packet) THEN
Discard the packet

Discard the packet

ENDIE

IF (the lengths of the Authentication Name and Authentication Data are not both zero or non-zero) THEN

Reinitialize the user's profile and set the profile state to Incomplete

```
ELSE IF (the opcode is Manage) THEN  
    IF (the Session ID does not match the Session ID recorded in the user's profile from the  
        Accept packet) THEN  
        Discard the packet  
ENDIF
```

305

210

210

```
IF (the Display Number does not match the Display Number recorded in the user's profile  
from the Request packet) THEN  
    Discard the packet  
ENDIF
```

```
IF (if the Display Class contains invalid characters) THEN  
    Discard the packet  
ENDIF
```

३००

IF (if the Display Class does not match any previous recorded Display Class for this user)

THEN
 Discard the packet
ENDIF

Set the user's profile state to Complete

ELSE IF (the opcode is Refuse) THEN
 IF (the Session ID does not match the Session ID recorded in the user's profile from the
 Accept packet) THEN
 Discard the packet
 ENDIF
 ENDIF

230
235

ELSE IF (the opcode is Failed) THEN
 IF (the Session ID does not match the Session ID recorded in the user's profile from the
 Accept packet) THEN
 Discard the packet
 ENDIF
 ENDIF

IF (the Status string is NOT composed of printable characters) THEN
 Discard the packet
ENDIF

Reinitialize the user's profile and set the profile state to Incomplete

ELSE IF (the opcode is KeepAlive) THEN
 IF (the X Display Number is invalid) THEN
 Discard the packet
 ENDIF

IF (the Display Number does not match the Display Number recorded in the user's profile
from the Manage packet) THEN

250

255 Discard the packet
 ENDIF

260 IF (the Session ID does not match the Session ID recorded in the user's profile from the Manage packet) THEN
 Discard the packet
 ENDIF

265 ELSE IF (the opcode is Alive) THEN
 IF (the Session Running flag is not 0 or 1) THEN
 Discard the packet
 ENDIF

270 IF (the Session Running flag is True) THEN
 IF (the Session ID does not match the Session ID recorded in the user's profile from the Manage packet) THEN
 Discard the packet
 ENDIF

275 ELSE – the Session Running flag is False
 IF (the Session ID is not zero) THEN
 Discard the packet
 ENDIF

280 Reinitialize the user's profile and set the profile state to Incomplete
 ENDIF

285 ELSE – the XDMCP Opcode is not allowed
 Discard the packet
 ENDIF

 ELSE – the XDMCP Opcode is being sent in the wrong direction
 Discard the packet
 ENDIF

	ELSE – the XDMCP Opcode is not on the allowed-opcodes list
	Discard the packet
ENDIF	
ELSE – the server port is not for the XDMCP protocol	
Discard the packet	
ENDIF	
ELSE – neither of the IP ports are on the allowed-ports list	
Discard the packet	
ENDIF	
295	
	ELSE IF (it is an IP/TCP packet) THEN
	IF (this packet is for an established TCP connection) THEN
	IF (the TCP RST flag is set) THEN
	Close this connection immediately
	ENDIF
	ENDIF
	IF (this is the last connection with this user) THEN
	Reinitialize the user's profile and set the profile state to Incomplete
	ENDIF
300	
	ELSE IF (the TCP FIN flag is set for the first time for this connection) THEN
	Remember that the FIN flag was set in the user's profile
	Record that the FIN flag was observed at the current date/time
	ENDIF
	ELSE – the packet is not for an established TCP connection
	IF (the packet TCP SYN flag is set and the TCP ACK flag is not set) THEN
	Check the source and destination ports against a list of allowed well-known
	ENDIF
305	
	IF (either port is on the allowed port list) THEN
	Check if the TCP connection is being opened in an allowed direction
	Check the source and destination ports against a list of allowed well-known
310	
	ENDIF
315	

IF (the TCP connection is being opened in an allowed direction) THEN
 Check if the user port is for the X-Windows protocol

320

```
IF (this is an X-Windows connection) THEN  
    IF (there is not an existing profile for this user) THEN  
        Discard the packet  
    ELSE – there is an existing profile for this user  
        IF (the state of the user's profile is not Complete) THEN  
            Discard the packet  
        ENDIF
```

330

If (the user port does not correspond to the X Display Number in the user's profile)

335

```
    Remember this connection in the user's profile
ELSE – the TCP connection is being opened in a disallowed direction
    Discard the packet
ENDIF

ELSE – neither of the IP ports are on the allowed-ports list
    Discard the packet
ENDIF

ELSE – this is not a TCP SYN packet
    Discard the packet
ENDIF

ENDIF
```

```

Discard the packet
ENDIF
ELSE – it is a non-IP packet
Discard the packet
ENDIF
355

```